REMARKS

The Examiner has rejected Claims 1, 5, 7-10, and 16-20 under 35 U.S.C. 102(e) as being anticipated by Wells (U.S. Patent No. 6,338,141 B1). Applicant respectfully disagrees with such rejection.

With respect to the independent claims, the Examiner has relied on the following excerpt from Wells to make a prior art showing of applicant's claimed "virus definition sentence comprising object code providing operations to detect the identified computer virus within a computer system" (see this or similar, but not necessarily identical language in the independent claims).

> "Having multiple, usable signatures for each virus is advantageous. It allows Raven to verify infections with a high degree of certainty and helps in the avoidance of false identifications. Although all of the relational data is available, not all of it is used in every case. Rather, a subset of specific critical data is often used. This allows Raven to maintain good verification, while also allowing it to easily recognize new variants of known viruses. Additionally, the data can be easily overridden or modified in various ways to enhance performance. Generally, however, the data are never modified. In fact, most of the data is never touched, or even seen, by the developer, because the Raven detection system is built almost entirely by an automated system." (Col. 2, lines 27-39 - emphasis added)

Applicant firmly asserts that the excerpt from Wells relied upon by the Examiner merely teaches a system that has "multiple, usable signatures for each virus [which]... allows Raven to verify infections with a high degree of certainty" (emphasis added). Applicant further notes that Wells teaches that when a "virus detection tool...is run on any given system...the gathered data for each file checked is tested against the relational data that represents the known viruses stored in the virus-detection database" (Col. 2, lines 54-60). Clearly, Wells only discloses virus signatures that are compared against data by a virus detection tool, but not that such virus signatures themselves include any sort of operations. Thus, such signatures do not even suggest "a virus definition sentence

comprising object code providing **operations** to detect the identified computer virus within a computer system" (emphasis added), as claimed by applicant.

In addition, with respect to the independent claims, the Examiner has relied on the following excerpt from Wells to make a prior art showing of applicant's claimed "virus removal sentence comprising object code providing operations to clean the identified computer virus from the computer system" (see this or similar, but not necessarily identical language in the independent claims).

> "Raven is first implemented as part of a virus analysis tool. This tool is run on a large collection of viruses. The virus collection must meet certain criteria and have a known format. The output from the analysis-implementation of Raven is then input to a build system that, in turn, outputs a virus-detection database or update to be that is used by the second implementation of Raven.
>
> Raven is implemented in this second form as part of a virus detection tool. When this tool is run on any given system (such as a user's system), the gathered data for each file checked is tested against the relational data that represents the known viruses stored in the virus-detection database. An exact match of all related data indicates a known virus is present. In addition, if most, but not all, of the data is matched, there is a high probability that an unknown (but closely related) virus is present.
>
> While a few viruses may still need to be examined by a virus researcher, most are analyzed and accepted automatically. The automated system produces over 90 percent of the data sets used by Raven. The automated system allows for rapid response for new viruses." (Col. 2, lines 47-67 - emphasis added)

Applicant respectfully asserts that the excerpt from Wells relied upon by the Examiner merely teaches outputting a virus-detection database and using the virus-detection database to identify viruses within data. For example, such excerpt from Wells merely discloses that when the virus detection tool "is run on any given system (such as a user's system), the gathered data for each file checked is tested against the relational data that represents the known viruses stored in the virus-detection database" (emphasis added). Clearly, the excerpt relied upon by the Examiner only relates to virus identification, and therefore in no way discloses "a virus removal sentence comprising

object code providing operations to clean the identified computer virus from the computer system" (emphasis added), as claimed by applicant.

Further, with respect to the independent claims, the Examiner has relied on the following excerpt from Wells to make a prior art showing of applicant's claimed "converter converting the virus definition records stored in the structured virus database into a virus data file comprising virus definition sets, each virus definition set comprising: binary data encoding instructions to detect the computer virus within a computer system, wherein the instructions comprise the object code to detect the identified computer virus" and "binary data encoding instructions to clean the computer virus from the computer system, wherein the instructions comprise the object code to clean the identified computer virus" (see this or similar, but not necessarily identical language in the independent claims).

> "In multiple changed files that appear anomalous were detected, isolated and the originals successfully restored, then the isolated samples are analyzed as a group by using the Raven function in its analysis mode. This is the mode that is used to produce virus signatures. If usable Information-structure-based signatures are generated they are added to the virus detection database. The anomalous files are also analyzed by comparison to the original files (restored in Step 8b) and, if possible, repair information is generated and added to the virus repair database. Note that..." (Col. 9, lines 58-67 - emphasis added)

Applicant respectfully asserts that the excerpt from Wells relied upon by the Examiner merely teaches that if "multiple changed files that appear anomalous were detected, isolated and the originals successfully restored, then the isolated samples are analyzed [and]...[i]f usable Information-structure-based signatures are generated they are added to the virus detection database" (emphasis added). Such excerpt further teaches that "[t]he anomalous files are also analyzed by comparison to the original files...and, if possible, repair information is generated and added to the virus repair database" (emphasis added).

Clearly such excerpt only relates to generating information-structure-based signatures and adding it to a virus detection database and generating repair information

and adding it to a virus repair database, where such information is generated from changed files. Applicant, on the other hand, claims "converting the virus definition records stored in the structured virus database" (emphasis added), as claimed.

In addition, applicant notes that Wells further teaches that "the system can be scanned with the new virus detection and repair information" (Col. 10, lines 10-12-emphasis added). Clearly scanning data with such virus detection and repair information, as in Wells, in no way discloses any sort of specific binary instructions, let alone applicant's specifically claimed "binary data encoding instructions to detect the computer virus within a computer system, wherein the instructions comprise the object code to detect the identified computer virus" and "binary data encoding instructions to clean the computer virus from the computer system, wherein the instructions comprise the object code to clean the identified computer virus" (emphasis added), as claimed by applicant.

Additionally, with respect to the independent claims, the Examiner has relied on Column 9, lines 58-67 from Wells, as excerpted above, to make a prior art showing of applicant's claimed "client anti-virus language decompiler converting each virus definition set in the virus data file into a virus definition record" (see this or similar, but not necessarily identical language in the independent claims).

Again, applicant respectfully asserts that the excerpt from Wells relied upon by the Examiner merely teaches that if "multiple changed files that appear anomalous were detected, isolated and the originals successfully restored, then the isolated samples are analyzed [and]...[i]f usable Information-structure-based signatures are generated they are added to the virus detection database" (emphasis added). Such excerpt further teaches that "[t]he anomalous files are also analyzed by comparison to the original files...and, if possible, repair information is generated and added to the virus repair database" (emphasis added).

However, the excerpt relied upon by the Examiner makes absolutely no disclosure of "a client anti-virus language decompiler converting each virus definition set in the

virus data file into a virus definition record" (emphasis added), as claimed by applicant. In Wells, a virus signature is simply generated from changed files, whereas applicant claims "converting each virus definition set in the virus data file into a virus definition record" where such virus definition set in the virus data file includes "instructions to detect the computer virus...[and] instructions to clean the computer virus" (see independent claims for context-emphasis added), in the context claimed by applicant. Clearly simply generating virus signatures does not meet applicant's claimed converting each virus definition set, as claimed. Only applicant claims a technique in which a virus definition set is converted.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Wells reference, as noted above. Thus, a notice of allowance or proper prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 5, the Examiner has relied on Column 9, lines 58-67 from Wells, as excerpted above, to make a prior art showing of applicant's claimed "server anti-virus language decompiler converting each virus definition set in the virus data file into a virus definition record."

Again, applicant respectfully asserts that the excerpt from Wells relied upon by the Examiner merely teaches that if "multiple changed files that appear anomalous were detected, isolated and the originals successfully restored, then the isolated samples are

analyzed [and]...[i]f usable Information-structure-based signatures are generated they are added to the virus detection database" (emphasis added). Such excerpt further teaches that "[t]he anomalous files are also analyzed by comparison to the original files...and, if possible, repair information is generated and added to the virus repair database" (emphasis added). Thus, in Wells the virus signatures are only generated from changed files, which clearly does not meet any sort of "server anti-virus language decompiler **converting** each virus definition set in the virus data file into a virus definition record" (emphasis added), as claimed by applicant.

Again, applicant respectfully asserts that the foregoing anticipation criterion has simply not been met by the Wells reference, as noted above. Thus, a notice of allowance or proper prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 21-24 below, which are added for full consideration:

"wherein each virus definition set further includes descriptive names corresponding to each computer virus" (see Claim 21);

"wherein each virus definition set includes a plurality of ordered virus definitions" (see Claim 22);

"wherein the plurality of virus definitions are ordered for optimal retrieval" (see Claim 23); and

"wherein the virus data file is encrypted" (see Claim 24).

Again, a notice of allowance or proper prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P376/00.140.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100